Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

Analysis and Implementation of New Technique Collaborated with Huffman Encoding and DNA

Uma Rani[1], Surjeet Dalal[2]
[1]World College of Technology and Management, Gurugram, Haryana
[2]Amity University Manesar, Gurugram, Haryana
[1]singh19uma@gmail.com; [2]profsurje etdalal@gmail.com

Abstract—***Security of information has become a key research area due to the enhancement in online data transfer rate. Data security can be employed using various ways such as cryptography, encryption, watermarking stenography, etc. Image stenography hides the secret message under a cover image to enhance security. Several techniques have been proposed which are used to implement the methodology of hiding data. This paper represented, analyzed, and implemented a new technique that collaborated with two other techniques such as Huffman encoding and DNA. Initially, data is encrypted, compressed, and then hidden under an image for an advanced level of security. The experimental analysis has been performed using two different formats of images such as JPEG and BMP of three images. The message bits are varying from 50 to 1000 for the evaluation. The results acquired from the evaluation concluded that the proposed technique outperforms the traditional technique in terms of PSNR and MSE.***

Keywords— Stenography, Embedding, Extracting, DNA, Huffman Encoding

I. INTRODUCTION

Stenography is a term that is developed by concatenating two of the Greek words i.e. “steganos” and “graphie” which denotes the “enclosed writing”. Together it alluded as shrouded (covered up or secured) the message. In 1499 first term was utilized by Johannes Trithemius in his Stegno-graphia. He had done his postulation in the area of cryptography and stenography and disguised it as a book on enchantment. Along these lines, the message that is covered up under the item is considered as spread which can be of anything for example pictures, articles, shopping records, or other spread content. [1] Therefore, it is a high-security method considered for long-term information transmission. Stenography is a step-by-step procedure to hide the message before sending it to the receiver. The hiding of the data can be performed by using any of the cover files. Here cover file refers to the file that is used for hiding the data behind it. The cover file can be an audio, text, video, image, etc. The intruders are not capable of finding the original meaningful data which is hidden behind the cover file. If stenography is applied with cryptography, it provides high data security to the information. The combination of stenography with cryptography is feasible by first applying encryption of the message using cryptography and then hiding the message using the Stenography process. In Figure 1 the procedure of stenography alongside cryptography appeared. In this Firstly the message and spread picture are chosen and afterward, the message is encoded by utilizing the private key by the sender afterward, the scrambled message is embedded on the spread picture which is additionally moved to the recipient by the sender of the correspondence. At the beneficiary end, the message is separated from the spread

Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

picture and afterward, the unscrambling of the message is finished by applying the mystery key shared by the sender [14]. Stenography is introduced to establish secure communication between sender and receiver without having any fear of hackers and attackers. Because of its points of interest, it has been utilized in a few territories including military, insight agents, or authorities. Stenography is further comprised of various techniques that are used specifically to secure the data before embedding it in the cover file so that the unauthenticated user does not have any access to the critical data. The principal objective of utilizing Stenography is to stay away from the consideration of the aggressor from the shrouded data in the transmitted as though the assailant would come to realize that there is concealed information in the sent message then the eyewitness will attempt every conceivable thought so he can peruse the concealed message.

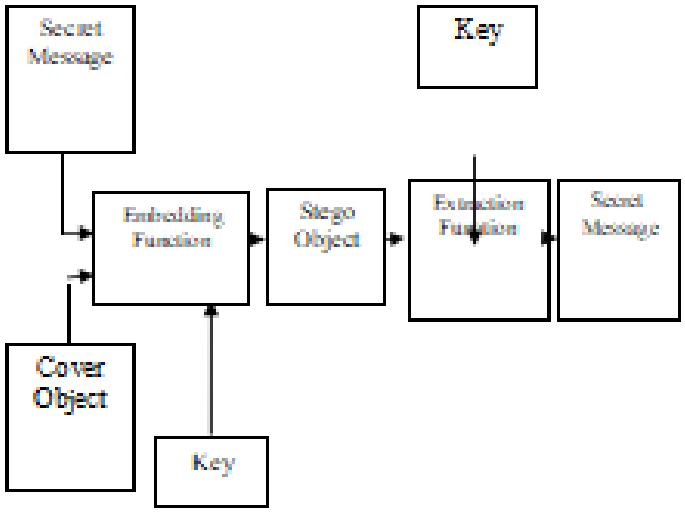


Figure 1. A model of the Stenography process with cryptography

II. BACKGROUND

Stenography is a procedure used to transmit a mystery message from a sender to a collector in a manner with the end goal that a potential interloper doesn't associate the presence with the message. By and large, this should be possible by installing the mystery message inside another computerized medium, for example, content, picture, sound, or video. The word Stenography is of Greek birthplace and signifies "hid expressing" from the Greek words steganos signifying "secured or ensured", and realistic signifying "composing". Security of the data is one of the major concerns. Various Stenography techniques have been proposed earlier but still, the required results were not achieved. Usually, watermarking techniques can be divided into two categories. The first category of watermarking belongs to spatial domain watermarking. In spatial domain watermarking the LSB technique is implemented. In the LSB technique, the data is hidden in the least significant bits

of the cover image pixels. However, this leads to a large amount of error and distortion in the cover image. Now the second category belongs to the transform domain watermarking. In the transform domain, techniques like discrete cosine transform (DCT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT) are implemented. In the transform domain, the data is hidden in frequency coefficients. As the human eyes can easily detect the variations in low-frequency components therefore the data hidden in low frequencies can be easily detected. Hence there is a requirement to develop such a technique that can be able to secure the data as well as least distortion should occur in the image after hiding the data.

III. PROPOSED WORK

To resolve the issues of the existing technique, a new method is proposed which is color image watermarking to hide the content of the image into the cover image. In the proposed technique, initially, the image is extracted from the database, and then encoding and compression of data is performed after that to hide the data color image watermarking technique is used. For the encoding purpose, a DNA algorithm is used and for compression as well as the encryption process Huffman coding technique is implemented. After that for hiding the data color watermarking is implemented. This technique is based on the DCT transform. In this technique, data is hidden in the luminance of the image by processing all the colors in the image. As the human eyes are less sensitive to any kind of variations in blue color therefore data is embedded in this color. It can accomplish a moderately high installing limit with no visual bending in the resultant stego picture. This work will likewise show the aggressive execution of the proposed framework in correlation with different frameworks.

IV. METHODOLOGY

The proposed method is divided into two parts data embedding process and extraction process. Initially, data was hidden and then extraction of data from the stego image was performed. The methodology of the proposed method is described below:

1 Embedding Process

The embedding process hides the secret message under the cover image using DNA and the Huffman encoding technique. The steps followed to embed the data are shown as:

(a) Initially read the cover image in which data will be hidden.
(b) Then convert the format of the cover image from RGB format to YCbCr format.
(c) Read a secret message to hide it under the image.
(d) Apply DNA encryption algorithm over the message to make it secure from unauthorized access.
(e) Now apply the Huffman encoding algorithm to compress the encrypted message under the cover image.
(f) Convert the secret message into binary format and then divide it into 8x8 blocks.
(g) Apply DCT to each acquired block.
(h) Employ quantization using a Quantization table and embed the message to the least significant bits of the quantized DCT coefficients of chosen frequency components.
(i) Finally applied Inverse DCT over the image and converted their format of YCbCr to RGB format.

(j) Acquire Stego Image.

2. Extraction Process

The second part of the proposed technique involves the extraction process where the message is extracted from the stego image. The methodology of the proposed extraction process is explained as:

(a) Read the Stego image of size NxM.
(b) Convert the image format of the stego image from RGB to YCbCr image format.
(c) Again divide the whole image into 8x8 blocks
(d) Then apply DCT to the individual block of the stego image
(e) Perform a quantization approach over the block.
(f) Extract the secret message from the cover image.
(g) Then apply the Huffman Encoding technique over the message to decompress the data.
(h) Then DNA encryption technique is applied to decrypt the message and convert it into a human-readable form.
(i) Acquire the recovered message.

The above figure depicts the process of data extraction where secret data is extracted from the stego image at the receiver end.

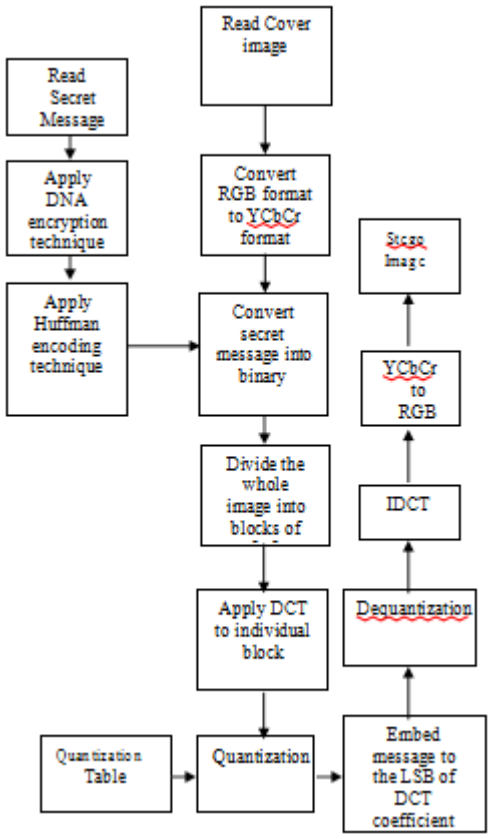


Figure 2 Data Embedding Process

Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

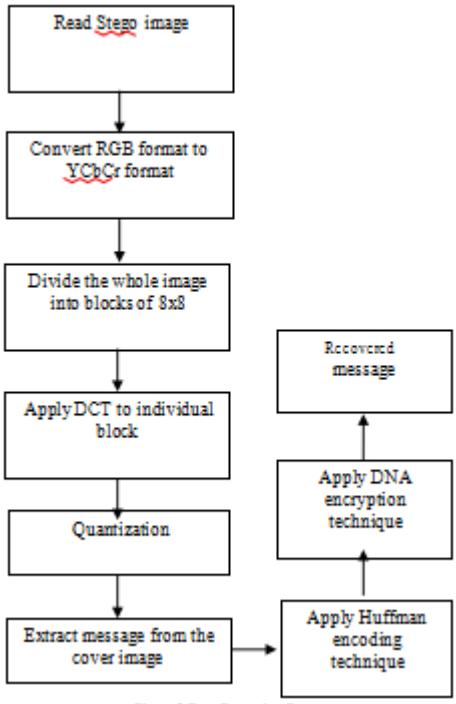
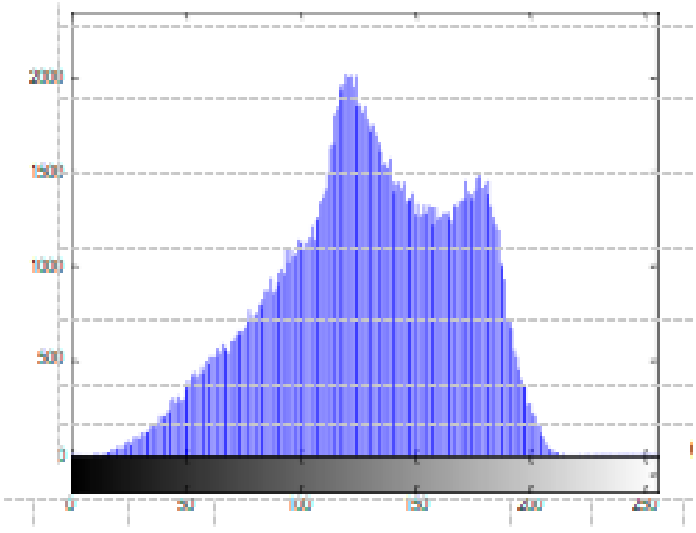


Figure 3 Data Extraction Process

V. RESULTS AND DISCUSSION

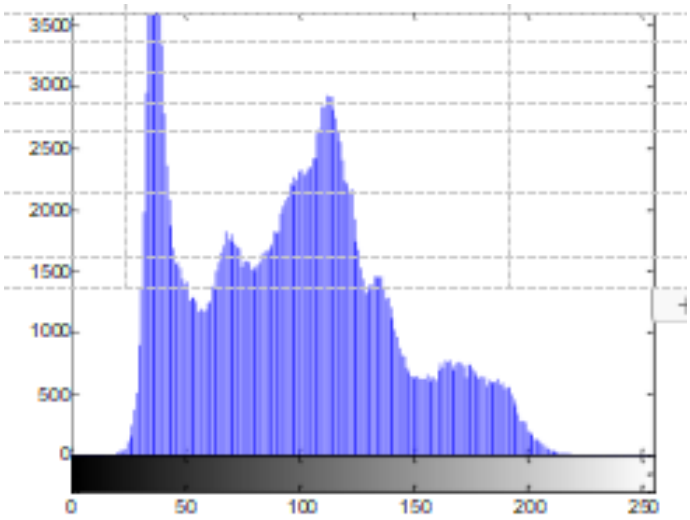
In this work, the proposed work is executed on three unique pictures by utilizing the variable measured message bit. A histogram is a graphical development of the appropriation of numerical information. It is an estimate of the likelihood conveyance of a steady factor. To construct a histogram, the initial step is to part the unblemished arrangement of qualities into an arrangement of interims and afterward check no. the qualities fall into interim. The interims must be adjoining, and are frequently of equivalent size. Picture histograms show the recurrence of pixels force esteems. In picture histograms, it has two tomahawks one is an x-pivot and the other is a y-hub. The x-pivot shows RGB level force and the y-hub shows the recurrence of these powers. The x-hub shows the scope of pixel esteems. The image below represents the histogram of the cover images i.e. Lena, Mandrill, and Flower. The x-axis ranges from 0 to 250 and the y-axis ranges from 0 to 2000 for the image of Mandrill and from 0 to 3500 for the image of Lena. The graph in Figure 5 shows the comparison of various techniques and proposed technique and proposed techniques by using the image of mandrill in terms of MSE (Mean Square Error). The Comparison is done between 1-LSB, 2-LSB, LF-DCT, MF-DCT, and DNA-Huffman (proposed technique). From the graph, it is observed that the y-axis represents the value of MSE that varies from 0 to 18 and the x-axis depicts the value for the message bit that ranges from 0 to 1000. The graph makes it clear that the proposed work has a better MSE (0.421) in comparison to others whereas the MF-DCT technique has the highest value for the MSE (16.23). The graph in Figure 6 shows the Peak Signal to noise ratio for the image of the mandrill by using different stenography techniques. The value of the PSNR is depicted by the y-axis

which ranges from 36 to 54 dB. The x-axis depicts the various message bits that start from 0 and end at 1000. The PSNR of the proposed work (52.1dB) is evaluated to be the highest value of PSNR among other mechanisms. The PSNR of the MF-DCT (38.02dB) is the lowest PSNR. The graph in Figure 7 shows the comparison of 4 techniques with the proposed technique concerning the peak signal-to-noise ratio for the image of Lena. The PSNR is measured in dB and handled by the y-axis and ranges from 30 to 55 dB. The x-axis in the graph calibrates the data in the terms of size of the message bit that is considered from 0 to 1000. The evaluated PSNR for the proposed work is 52.09 dB which is the highest one when compared to other techniques. The lowest PSNR is evaluated in LF-DCT technique i.e. 33.61dB. The graph of Figure 8 represents the mean square error regarding the image of Lena by using various techniques such as 1-LSB, 2-LSB, LF-DCT, MF-DCT, and the proposed technique i.e. DNA-Huffman. The comparison is done to evaluate the best among the defined techniques in terms of mean square error. The graphs make it clear that the least MSE is evaluated in the proposed work i.e. 0.41 and the highest mean square error is evaluated for LF-DCT i.e. 28.63. The highest value of the MSE shows that the level of performance is quite low; hence it is mandatory to have the lowest MSE to achieve reliable output. Figure 9 shows the graph that compares the MSE of the image of a flower that is observed by implementing the various stenography techniques. It is evaluated that the MSE of the proposed work is evaluated to be 0.41 which is the lowest one and the MSE for LF-DCT is 6.4 which is the highest one. The graph in Figure 10 shows the PSNR for the image of the flower by using various stenography techniques. The graph presents that the PSNR of the proposed work is the best PSNR observed at 52.13 and the worst PSNR observed for LF-DCT is 40.0

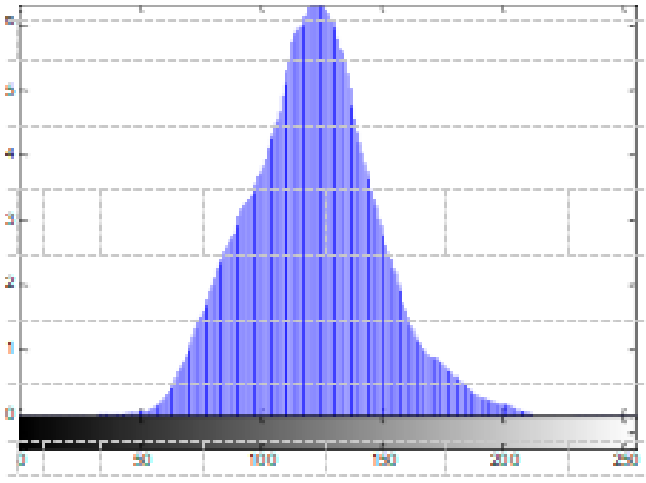


(a) Mandrill

Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024



(b) Lena



C. Flower

Figure 4 Histogram of cover images.

Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

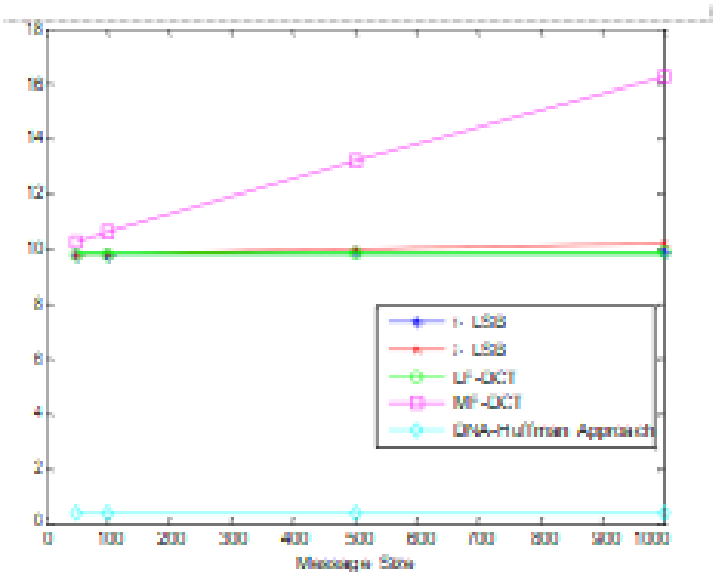


Figure 5 MSE for the image of mandrill

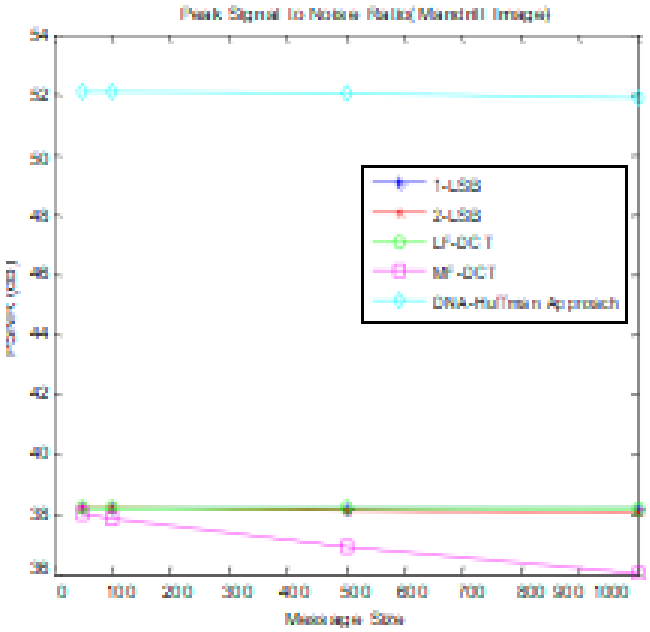


Figure 6 PSNR for the image of mandrill

Engineering and Technology Journal for Research and Innovation (ETJRI)
ISSN 2581-8678, Vol. VI, Issue II, Jul 2024

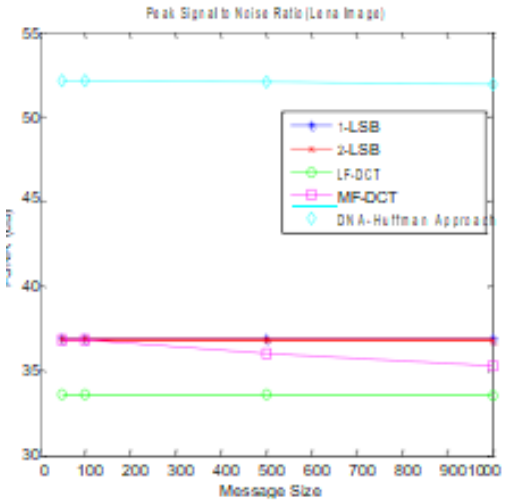


Figure 7 PSNR for the image of Lena

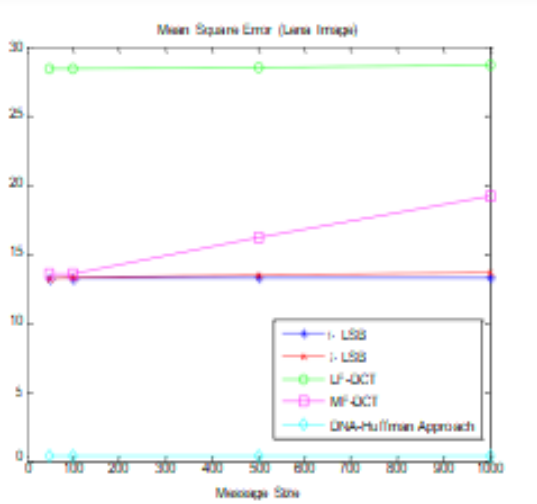


Figure 8 MSE for the image of Lena

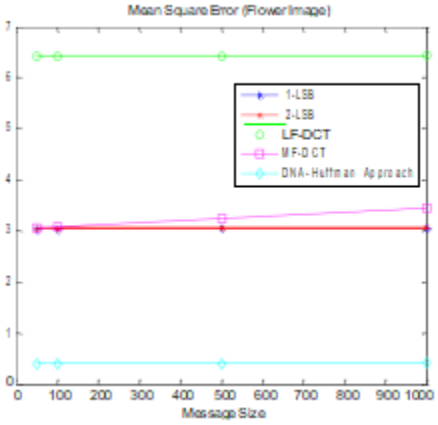


Figure 9 MSE for the image of Flower

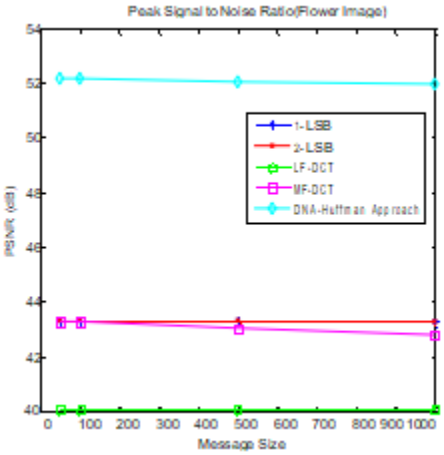


Figure 10 PSNR for the image of Flower

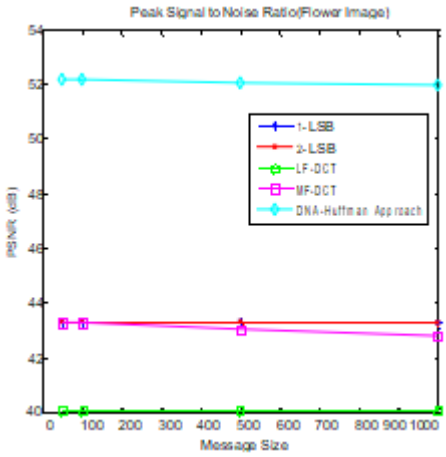


Figure 10 PSNR for the image of Flower by using various techniques and proposed work

VI. CONCLUSION

Image stenography techniques have been used to embed the secret message using a cover image. Similarly, the proposed technique has performed stenography using two different approaches such as DNA and Huffman encoding. Primarily, the DNA technique is used to hide and decrypt the data under an image whereas Huffman encoding is used for compression as well as decompression of the encrypted secret message. Using the proposed approach, simulation analysis has been performed that surpasses the traditional 1-LSB, 2-LSB, LF-DCT, and MF-DCT techniques. The comparison has been performed based on different performance parameters such as PSNR and MSE. The DCT algorithm provides neutral results and has less distortion. Moreover, the proposed technique results in high PSNR and low MSE value which means that the former technique has less distortion and a high level of security.

The proposed technique is collaboratively using two different approaches such as DNA and Huffman for encryption and compression respectively. In the future, this technique can be extended using swarm intelligence optimization algorithms where an optimization algorithm can be used to evaluate the best location given hiding the secret data under a cover image.

REFERENCES

[1]. R.Poornima, "An Overview Of Digital Image Stenography", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1, Pp 23 -31

[2]. J. K. Mandal (2012) "Colour Image Stenography Based on Pixel Value Differencing in Spatial Domain" International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, Pp 83-93

[3]. A Rashi Singh (2014), "Review on Image Stenography" International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, Volume 4, Issue 5, Pp 686-689

[4]. Anil Kumar (2013), "A Secure Image Stenography Based on RSA Algorithm and Hash-LSB Technique" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, Pp 363-372

[5]. Vinay Pandey, Manish Shrivastava "Medical Image Protection using stenography by crypto image as cover Image", International Journal of Advanced Computer Research, VOL 2, Issue 5, 2012

[6]. Madhu B., Ganga Holi, Srikant Murthy K. "An Overview of Image Security Techniques", International Journal of Computer Applications, Vol 154, 2016.

[7]. Mamta Jain, "Secure Medical Image Stenography with RSA Cryptography using Decision Tree", IEEE 2017

[8]. Swati Malik, Ajit "Securing Data by Using Cryptography with Stenography", 2013

[9]. Rani, U., Kumar, S., Dahiya, N. et al." An optimized neural network with AdaHessian for crypto-jacking attack prediction for Securing Crypto Exchange Operations of MEC applications." J Cloud Comp 13, 63 (2024). https://doi.org/10.1186/s13677-024-00630-y

[10]. Rani U, Dahiya N, Sharma YK," Hyper-parameter tuned deep learning approach for effective human monkeypox disease detection." Sci Rep. 2023 Sep23;13(1):15930.Scientific Reports, Impact Factor 4.9(2023) https://doi.org/10.1038/s41598-023-43236-1

[11]. Monika Patel, Priti Srinivas Sajja," Analysis and Survey of Digital Watermarking Techniques" IJARCSSE, Vol 3, Pp 203-210, 2013

[12]. Atallah M (2012)," A New Method in Image Stenography with Improved Image Quality" Applied Mathematical Sciences, Vol. 6, 2012, no. 79

[13]. Rani, U., Kumar, S., Dahiya, N. et al "An Efficient Brain Tumor Segmentation Method Based on Adaptive Moving Self-Organizing Map

and Fuzzy K-Mean Clustering;" Sensors, Impact factor 3.9(2023)

[14]. Mohamed M. Fouad, "Enhancing the imperceptibility of image stenography for information hiding", Computer Science and Information Systems (FedCSIS), Federated Conference on September 2017